UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,713	12/11/2003	Clark Debs Jeffries	END920030137US1	8632

37945 7590 11/21/2007

DUKE W. YEE
YEE AND ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
11/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action After the Filing of an Appeal Brief	Application No. 10/733,713	Applicant(s) JEFFRIES ET AL.	
	Examiner Harris C. Wang	Art Unit 2139	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

The reply filed 12 November 2007 is acknowledged.

1. ☐ The reply filed on or after the date of filing of an appeal brief, but prior to a final decision by the Board of Patent Appeals and Interferences, will not be entered because:

   a. ☐ The amendment is not limited to canceling claims (where the cancellation does not affect the scope of any other pending claims) or rewriting dependent claims into independent form (no limitation of a dependent claim can be excluded in rewriting that claim). See 37 CFR 41.33(b) and (c).

   b. ☐ The affidavit or other evidence is not timely filed before the filing of an appeal brief. See 37 CFR 41.33(d)(2).

2. ☐ The reply is not entered because it was not filed within the two month time period set forth in 37 CFR 41.39(b), 41.50(a)(2), or 41.50(b) (whichever is appropriate). Extensions of time under 37 CFR 1.136(a) are not available.

   Note: This paragraph is for a reply filed in response to one of the following: (a) an examiner's answer that includes a new ground of rejection (37 CFR 41.39(a)(2)); (b) a supplemental examiner's answer written in response to a remand by the Board of Patent Appeals and Interferences for further consideration of rejection (37 CFR 41.50(a)(2)); or (c) a Board of Patent Appeals and Interferences decision that includes a new ground of rejection (37 CFR 41.50(b)).

3. ☒ The reply is entered. An explanation of the status of the claims after entry is below or attached.

4. ☒ Other: *The status of the claims remain rejected, because the arguments were not found to be persuasive. The Examiner contends that adding the Diffie-Hellman key agreement to Peyravian would have been obvious to one of ordainary skill in the art, using known methods to achieve predictable results. In particular, the Figures 2 and 3 of Peyravian match up closely to Figures 4 and 6 of the instant application, with the exception of the inclusion of the terms (p,g ,g^x, g^y). The Diffie-Hellman key exchange is a well known method for authentication described in detail in the now expired patent (4200770) where the large prime number p and the integer g that is a primative root of p are used in conjunction with the private values x and y in order to calculate a shared secret.*
The Applicant argues that "the present invention, the Diffie-Hellman key agreement scheme is used by the client and server to establish a shared secret to protect exchanges; and the method of the present invention does not use static or established Diffie-Hellman ephemerals between the client and the server. To the contrary, Trostle's method uses two publicly known numbers (pg. 12 of Remarks)." Although traditionally in the DH key exchange p and g are public numbers, even if p and g are sent privately (which is not disclosed in the instant application), the functionality of the DH-key exchange is still the same. In other words, because the privacy of p and g are not important in DH-key exchange, assuming arguendo, even if Trostle teaches a public p and g and the instant application teaches a private p and g, it does not change the fact that the Applicant is using the Diffie-Hellman key exchange,a well known method, for authenticaiton which would have achieved predictable results..

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100